UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,004	02/02/2004	Mark J. Dickelman	JPC-056-OR1	2003

70813 7590 07/09/2009

GOODWIN PROCTER LLP
901 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20001

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
07/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

AAlpha-Kpetewama@goodwinprocter.com
patentdc@goodwinprocter.com

Office Action Summary	Application No.	Applicant(s)	
	10/708,004	DICKELMAN ET AL.	
	Examiner	Art Unit	
	TRANG DOAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 03/18/2009.

2. Claims 1, 5, 7, 9-11, 13-14, 17, 19-20, 23, 26, 30, 32, 34-37, 40 and 42 have amended.

3. Claims 1-42 are pending for consideration.

Response to Arguments

4. Applicant's arguments filed on 03/17/2009 have been fully considered but they are not persuasive.

5. Applicant argues on page 22 of the Remarks that Solaris never mentions a proxy server or even uses the word proxy anywhere in its disclosure. Examiner respectfully disagrees. Solaris discloses the trusted Solaris 8 operating environment provides methods for limiting external access, as well as extensive internal protection against intruders and misuse that is equivalent to the proxy server recited in claim 1 (see Solaris: pages 2-3).

6. Applicant further argues that none of the recited references teach or suggest a top-down security design that limits communication among a plurality of compartments as presently claimed. Examiner respectfully disagrees. Solaris does teach a plurality of compartments which is used to protect the information from unauthorized access (see Solaris: pages 23-24).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-3, 6-9, 11-12, 14-16, 19, 22, 26-28, 34-37 and 39 are rejected under 35 U.S.C. 102(b) as being anticipated by (Trusted Solaris 8 Operating Environment) (hereinafter Solaris).

Regarding claim 1, Solaris discloses a network computer system for providing security, wherein the network computer system comprises: a monitoring function for the network computer system (Solaris: page 16, paragraphs 2-4); at least one outside server for an untrusted computer network, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one outside server for the untrusted computer network; at least one proxy server, wherein the at least one outside server for the untrusted computer network is able to read and write data to the at least one proxy server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one proxy server (Solaris: page 17, paragraph 2); at least one inside server, wherein the at least one proxy server is able to read and write data to the at least one inside server, wherein the monitoring function can read and execute data from, but cannot write data to, the at least one inside server; and a core operating system that is a portion of an operating system, wherein the at least one outside server,

the at least one proxy server and the at least one inside server can read and execute data from, but cannot write data to, the core operating system (Solaris: page 18, paragraph 3-5; page 21, paragraphs 1-2; and pages 22-24).

Regarding claims 2 and 27, Solaris discloses wherein the monitoring function includes at least one system level auditing function (Solaris: page 18, paragraph 6).

Regarding claims 3 and 28, Solaris discloses wherein the at least one system level auditing function resides within a first compartment and the at least one system level auditing function transports system log protocol events, generated by the operating system, through the network computer system without providing access to the system log protocol events from the at least one outside server, the at least one proxy server and the at least one inside server (Solaris: page 18, paragraph 6).

Regarding claim 6, Solaris discloses wherein the monitoring function includes at least one system health monitoring tool (Solaris: page 22, paragraph 3).

Regarding claim 7, Solaris discloses wherein the at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the network computer system, and the fifth compartment includes source code for the system health monitoring tool,

wherein the fourth compartment can read and execute data from, but cannot write data to, the fifth compartment (Solaris: page 22, paragraph 3).

Regarding claim 8, Solaris discloses wherein the monitoring function includes at least one integrity check system (Solaris: page 22 and page 23).

Regarding claims 9 and 34, Solaris discloses wherein the at least one integrity check system resides within a sixth compartment and a seventh compartment, wherein the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment includes source code for the integrity detection system, wherein the sixth compartment can read and execute the source code from, but cannot write data to, the seventh compartment (Solaris: page 22 and page 23).

Regarding claims 11 and 35, Solaris discloses wherein the at least one outside server includes at least one eighth compartment where outside requests are received, processed, and then passed to the at least one proxy server for further processing and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the core operating system (Solaris: pages 22-24).

Regarding claim 12, Solaris discloses wherein the source code includes encryption binaries and configuration files (Solaris: page 19, paragraph 4).

Regarding claims 14, 36 and 39, Solaris discloses wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server, which are then passed to the at least one inside server for further processing and at least one eleventh compartment wherein source code for the at least one proxy server resides, where the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the core operating system (Solaris: pages 22-24).

Regarding claim 15, Solaris discloses wherein the source code includes binaries and configuration files (Solaris: pages 22-24).

Regarding claim 16, Solaris discloses wherein the at least one proxy server makes buffer checks and file extension requests to ascertain whether a security threat is present (Solaris: pages 22-24).

Regarding claims 19 and 37, Solaris discloses wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all requests received from the untrusted computer network that have been screened and deemed valid for further processing and at least one thirteenth compartment where source code for the at least one inside server resides, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment and the at least one thirteenth compartment can read and execute data from, but cannot write data to, the core operating system (Solaris: pages 22-24).

Regarding claim 22, Solaris discloses wherein external data received from the outside through an untrusted computer network can pass from the at least one outside server wherein data from the at least one outside server can be read and written to the at least one proxy server, wherein data from the at least one proxy server can be read and written to the at least one inside server, wherein data from can at least one inside server can be read and written to at least one software application for further processing (Solaris: page 18, paragraph 3-5; page 21, paragraphs 1-2; and pages 22-24).

Regarding claim 26, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 4-5, 10, 13, 17-18, 20-21, 23-25, 30-33, 38 and 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Solaris in view of Sheikh et al. (US 2002/0078382) (hereinafter Sheikh).

Regarding claims 4 and 29, Solaris does not explicitly disclose wherein the monitoring function includes at least one intrusion detection system. However, Sheikh discloses wherein the monitoring function includes at least one intrusion detection system (Sheikh: paragraphs 0005, 0007 and 0011). Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in Solaris the feature of Sheikh as discussed above because a problem exists in the security software field because companies need to have security software that has the ability to monitor various aspects of the network and allow for forensic analysis when a breach or problem does occur (Sheikh: paragraph 0009).

Regarding claim 5, Solaris does not explicitly disclose wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known

patterns that may indicate an attack on the network computer system and the third compartment includes source code for the intrusion detection system, wherein the second compartment can read and execute data from, but cannot write data to, the third compartment (Sheikh: paragraphs 0011, 0034, 0076, 0078 and 0083). The same motivation was utilized in claim 4 applied equally well to claim 5.

Regarding claims 10, 30-32, 38 and 41, Solaris does not disclose first compartment, second compartment, third compartment, fourth compartment, fifth compartment, sixth compartment and seventh compartment which will be used as monitoring functions for network computer system. However, Sheikh discloses first compartment, second compartment, third compartment, fourth compartment, fifth compartment, sixth compartment and seventh compartment which will be used as monitoring functions for network computer system (Sheikh: paragraphs 0011, 0034, 0076, 0078 and 0083). Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in Solaris the feature of Sheikh as discussed above because a problem exists in the security software field because companies need to have security software that has the ability to monitor various aspects of the network and allow for forensic analysis when a breach or problem does occur (Sheikh: paragraph 0009).

Regarding claims 13 and 33, Solaris as modified discloses wherein the outside server includes at least one eighth compartment where outside requests are received,

processed, and then passed to the at least one proxy server for further processing and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from, but cannot write data to, the at least one core operating system that resides in a fourteenth compartment and the third compartment of the intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one check function can read and execute data from, but cannot write data to, the at least one eighth compartment for the at least one outside server (Sheikh: paragraphs 0011, 0034, 0076, 0078 and 0083). The same motivation was utilized in claim 4 applied equally well to claims 13 and 33.

Regarding claim 17, Solaris as modified discloses wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server which are then passed to the at least one inside server for further processing and at least one eleventh compartment where source code for the at least one proxy server resides, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the core operating system, residing in a fourteenth compartment, and the third compartment of the at least one intrusion

detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one tenth compartment for the at least one proxy server (Sheikh: paragraphs 0011, 0034, 0076, 0078 and 0083). The same motivation was utilized in claim 4 applied equally well to claim 17.

Regarding claim 18, Solaris as modified discloses wherein the source code includes binaries and configuration files (Sheikh: paragraphs 0011 and 0032). The same motivation was utilized in claim 4 applied equally well to claim 18.

Regarding claim 20, Solaris as modified discloses wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all requests received from the untrusted computer network have been screened and deemed valid for further processing and at least one thirteenth compartment where binaries and configuration files for the at least one inside server reside, wherein the at least one thirteenth compartment can read and execute data from, but cannot write data to, the core operating system, residing in a fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one twelfth compartment for the at least one inside server (Sheikh:

paragraphs 0011, 0034, 0076, 0078 and 0083). The same motivation was utilized in claim 4 applied equally well to claim 20.

Regarding claim 21, Solaris as modified discloses wherein system log protocol events produced by external devices can be forwarded through the at least one outside server, the at least one proxy server, and the at least one inside server to at least one other software application that monitors security intrusions (Sheikh: paragraphs 0011, 0034, 0076, 0078 and 0083). The same motivation was utilized in claim 4 applied equally well to claim 21.

Regarding claim 23, Solaris discloses a network computer system for providing security, wherein the network computer system comprises: at least one system level auditing function, wherein the at least one system level auditing function resides within a first compartment and the at least one system level auditing function transports system log protocol events produced by an operating system through the network computer system (Solaris: pages 22-24);

Solaris does not explicitly disclose at least one intrusion detection system, wherein the at least one intrusion detection system resides within a second compartment and a third compartment, wherein the second compartment monitors activity and makes comparisons to known patterns that may indicate an attack on the network computer system and the third compartment is where source code for the intrusion detection system resides, wherein the second compartment can read and

execute data from, but cannot write data to, the third compartment; at least one system health monitoring tool, wherein the at least one system health monitoring tool resides within a fourth compartment and a fifth compartment, wherein the fourth compartment monitors health and response time for the at least one outside server, the at least one proxy server and the at least one inside server and the fifth compartment is where source code for the system health monitoring tool resides, wherein the fourth compartment can read and execute data from, but cannot write data to, the fifth compartment; at least one integrity check system, wherein the at least one integrity check system resides within a sixth compartment and a seventh compartment, wherein the sixth compartment will provide an integrity check function to monitor changes to a baseline configuration of the network computer system and the seventh compartment is where source code for the integrity check system resides, wherein the sixth compartment can read and execute the source code from, but cannot write data to, the seventh compartment; at least one core operating system, residing within a fourteenth compartment; at least one outside server for an untrusted computer system, wherein the outside server includes at least one eighth compartment where outside requests are received and processed and at least one ninth compartment where source code for the at least one outside server resides, wherein the at least one eighth compartment can read and execute data from, but cannot write data to, the at least one ninth compartment and the at least one ninth compartment can read and execute data from the at least one core operating system that resides in the fourteenth compartment and the third compartment of the at least one intrusion detection function, the fifth

compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one outside server; at least one proxy server, wherein the at least one proxy server includes at least one tenth compartment where the at least one proxy server executes and filters requests from the at least one outside server and at least one eleventh compartment where source code for the at least one proxy server resides, wherein the at least one tenth compartment can read and execute data from, but cannot write data to, the at least one eleventh compartment and the at least one eleventh compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one proxy server; and wherein the at least one inside server includes at least one twelfth compartment where the at least one inside server executes all and requests received from the unsecured computer network have been screened and deemed valid for further processing by the at least one proxy server and at least one thirteenth compartment where source code for the at least one inside server resides, wherein the at least one twelfth compartment can read and execute data from, but cannot write data to, the at least one thirteenth compartment and the at least one thirteenth compartment can read and execute data from, but cannot write data to, the at least one core operating system, residing in the fourteenth

compartment, and the third compartment of the at least one intrusion detection function, the fifth compartment of the at least one system health monitoring tool and the seventh compartment of the at least one integrity check function can read and execute data from, but cannot write data to, the at least one inside server.

However, Sheikh discloses second compartment through fourteenth compartment as described above (Sheikh: paragraphs 0005, 0007 and 0011). Therefore, It would have been obvious to a person skilled art at the time the invention was made to have included in Solaris the feature of Sheikh as discussed above because a problem exists in the security software field because companies need to have security software that has the ability to monitor various aspects of the network and allow for forensic analysis when a breach or problem does occur (Sheikh: paragraph 0009).

Regarding claim 24, this claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

Regarding claim 25, this claim has limitations that is similar to those of claim 22, thus it is rejected with the same rationale applied against claim 22 above.

Regarding claim 40, this claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

Regarding claim 42, Solaris as modified discloses reading and writing data from the at least one inside server to at least one software application for further processing (Solaris: pages 22-24).

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431